UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,543	04/23/2007	Ofir Arkin	ARKIN2	3198

1444 7590 01/04/2010

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
SEKUL, MARIA LYNN	

ART UNIT	PAPER NUMBER
2461	

MAIL DATE	DELIVERY MODE
01/04/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/580,543	ARKIN, OFIR	
	Examiner	Art Unit	
	MARIA L. SEKUL	2461	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-73* is/are pending in the application.

4a) Of the above claim(s) *1-46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *47-73* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 May 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

Claims 47-73 are pending. Claims 1-46 were previously cancelled.

Response to Arguments

1. Applicant's arguments filed 09/08/2009 have been fully considered but they are not persuasive.

2. Applicant argues several points in which Rowland et al. does not apply to the present invention. Particularly, Applicant argues that Rowland et al. discloses a method and system for reducing the false alarm rate of a network intrusion detection system (NIDS) and does not perform passive deducing of information from network traffic, among other shortcomings of the Rowland et al. reference.

3. Examiner respectfully disagrees. Briefly, Rowland discloses a Passive Analysis Tool working in conjunction with the NIDS. The Passive Analysis Tool detects hosts in the target network prior to invoking NIDS monitoring on data sent to the host. The Passive Analysis Tool passively monitors the DHCP traffic sent to/from the DHCP server. After detecting a host, the Passive Analysis Tool performs OS and port fingerprinting on the target device. Specifically, Rowland et al. must identify the hosts on the network and have information regarding the hosts before NIDS can detect intrusion at the host. Therefore, Rowland et al. is particularly applicable to the present invention, as applied in the prior art rejections herein.

4. Prior § 101 rejections as to claims 47-63 and prior § 112 rejections as to claims 48, 63, 64 and 68 are withdrawn based on Applicant's responsive amendment.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. **Claim 68** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to **claim 68**, the claim recites the limitation " said received data " in line 6. There is insufficient antecedent basis for this limitation in the claim. The claim recites in lines 3-4, "giving rise to the detected data" to reference the immediately preceding limitation "receive data". The term "detected data" is not used subsequently in the claim, whereas "said received data" is recited in line 6.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. **Claim 47-52, 57-58, 63-68, and 70-73** are rejected under 35 U.S.C. 102(e) as being anticipated by **Rowland et al. (US PGPub US2003/0212910)** (hereinafter Rowland).

As to **claims 47, 72 and 73**, Rowland discloses a method, program storage device and computer program product for "detecting, substantially in real-time, data conveyed by one or more detected nodes operating in the communication network in a manner that is transparent to said one or more detected nodes, giving rise to the detected data, thereby detecting said data passively (passive analysis tool 110 monitors a dynamic host configuration protocol (DHCP) server to detect the dynamic addition of hosts to a protected network 104 by monitoring the lease activity ("detected data") between the host ("detected node") and the DHCP server, **Fig. 4; ¶ 34-38**; the OS and port fingerprinting mechanisms also perform a passive analysis of a target host to collect information on the host, **¶ 24-25**); and

"analyzing said detected data for identifying nodal information relating to the one or more detected nodes" (Rowland discloses analyzing the data to determine the target address ("nodal information") of a host ("detected node"), then determines if the operating system information for the host is known or not; **Fig. 4, ¶ 36**); and

nodal information relating to said communication network (data is analyzed to determine the target address ("nodal information") of a host ("detected node"), **Fig. 4; ¶ 36**; the IP address of the host is implicitly information relating to the protected network);

missing information regarding at least one of said one or more detected nodes (the target address of the detected host is used to determine if the operating system fingerprint is stored in the system cache; if it is not available ("missing information"), the OS fingerprint is obtained, **¶ 37**); and

"missing information regarding said communication network" (the operating system fingerprint of the detected host is implicitly information regarding the communication network as it pertains to a host in the protected network); and

"storing at least a part of the identified information on a storage device comprising a computer readable medium accessible thereto" (the passive analysis tool may store entries for a user defined length of time, **¶ 37**; passive offline fingerprinting mechanism 208 may store this information in a suitable storage location for later retrieval and use, **¶ 25**; it is anticipated that the storage location may be a storage device with a computer readable medium being accessible) ;

"querying at least one of one or more nodes operating in said communication network for said missing information provided at least partially from said storage device, giving rise to the queried nodes, thereby collecting said missing information actively" (Rowland discloses if the target host address is known in the system cache ("storage device"), the operating system (OS) fingerprint of the target host is obtained, which consists of sending IP packets at the target host (that is, querying the target host actively), **¶ 36**; *see also* **¶ 24** describing OS fingerprinting method).

As to **claim 48**, Rowland discloses all of claim 47 and further discloses:

"receiving additional data relating to the communication network" (Rowland discloses port fingerprinting mechanism that obtains port activity of a target host; **Fig; 2, ¶ 25**) ; and

"analyzing said additional data for identifying the missing information" (Rowland analyzes the data to determine whether a specific port is active or inactive"; **¶ 25**).

As to **claim 49**, Rowland discloses all of claim 47.

Rowland further discloses "nodal information comprises operating system information relating to operating systems operating on the one or more nodes" (Rowland discloses using the operating system fingerprinting result to determine the operating system of a target host; **Fig. 4, ¶ 37**).

As to **claim 50**, Rowland discloses all of claim 49.

Rowland further discloses "the nodes are included in at least one of the following: detected nodes and queried nodes" (Rowland discloses that either the target host is known ("detected node") and if it is not known, it is obtained, that is, the node is queried to supply the missing information ("queried node"); **¶ 36-37**).

As to **claim 51**, Rowland discloses all of claim 49 and further discloses "detection of the data comprises detecting at least one type of message from a group comprising DHCP (Dynamic Host Configuration Protocol) messages and SYN packets" (Rowland discloses passively monitoring a DHCP server and detecting DHCP packets/messages, **Fig. 4; ¶ 34**).

As to **claim 52**, Rowland discloses all of claim 49 and further discloses:

"receiving data corresponding to data conveyed by a detected node, giving rise to the received data (Rowland discloses obtaining OS fingerprint information from a target host which has been detected, **¶ 37**);

"inspecting said received data for one or more characteristics of a known operating system" (the OS fingerprinting mechanism analyzes the detected data to determine the operating system, **¶ 30**); and

"if inspecting said received data reveals that the data conforms with said one or more characteristics, indicating that the known operating system operates on the detected node" (Rowland determines the OS type and stores this information for the target host, **¶ 30**).

As to **claim 57**, Rowland discloses all of claim 47 and further discloses:

"generating a query message corresponding to the missing information for conveying said query message to one or more nodes to be queried" (Rowland discloses obtaining the operating system fingerprint (**¶ 37**) by sending IP packets to the target address with the expectation of a response (**¶ 24**), also referred to as sending a "query" message (*see*, **¶ 6**);

conveying the query message to said one or more nodes, giving rise to the queried nodes (IP packets are sent to the target with the expectation of a response (**¶ 24**), also referred to as sending a "query" message (*see*, **¶ 6**).

As to **claim 58**, Rowland discloses all of claim 57 and further discloses:

"receiving at least one response that corresponds to the query message" (Rowland discloses obtaining data from the target host during OS fingerprinting in response to sending IP packets to the host,; **¶ 37**); and

"processing the at least one response to retrieve information corresponding to the missing information" (Rowland sends queries to a target host during OS fingerprinting and obtains information in response to determine the operating system, **¶ 17**).

As to **claim 63**, Rowland discloses all of claim 57.

Rowland further discloses "the detected nodes comprise at least one queried node, and the data conveyed by detected nodes includes at least one response that corresponds to the query message". It is implicit in Rowland that a detected node includes a queried node because if the operating system of the detected node is not known, it will be queried to obtain the OS fingerprint (**¶ 36**). Therefore, the detected node will also be a queried node. It is further implicit that a response will be received from the detected node as part of the OS fingerprinting mechanism.

As to **claim 64**, Rowland discloses a network information collector comprising:

"a network detector for configured to detect, substantially in real-time, data conveyed by one or more detected nodes operating in the communication network in a manner that is transparent to the one or more detected nodes, giving rise to the detected data, thereby detecting said data passively" (passive analysis tool 110 monitors a dynamic host configuration protocol (DHCP) server to detect the dynamic addition of hosts ("substantially in real-time") to a protected network 104 by monitoring the lease activity ("detected data") between the host ("detected node") and the DHCP server, **Fig. 4; ¶ 34-38**; the OS and port fingerprinting mechanisms also perform a passive analysis of a target host to collect information on the host, **¶ 24-25**));

"an analyzer configured to analyze said detected data for identifying: nodal information relating to said one or more detected nodes (Rowland discloses analyzing the data to determine the target address of a host, then determines if the operating system information for the host is known or not; **Fig. 4, ¶ 36**);

nodal information relating to said communication network (data is analyzed to determine the target address ("nodal information") of a host ("detected node"), **Fig. 4; ¶ 36**; the IP address of the host is implicitly information relating to the protected network);

missing information regarding at least one of said one or more detected nodes (after determining the target address ("nodal information") of a host ("detected node"), the passive analysis tool determines if the operating system information for the host is known or not ("missing information"); **Fig. 4, ¶ 36**); and

missing information regarding said communication network (the missing operating system fingerprint of the detected host described above is implicitly information regarding the communication network as it pertains to a host in the protected network); and

a query engine configure to query at least one of one or more nodes operating in said communication network for said missing information, giving rise to the queried nodes, thereby collecting said missing information actively (Rowland discloses if the target host address is known in the system cache ("storage device"), the operating system (OS) fingerprint of the target host is obtained, which consists of sending IP packets at the target host (that is, querying the target host actively), **¶ 36**; *see also* **¶ 24** describing OS fingerprinting method).

As to **claim 65**, Rowland discloses all of claim 64.

Rowland further discloses "an input device configured to receive additional data relating to the communication network" (Rowland discloses a port fingerprinting

mechanism for querying for additional data port activity of a target host and receiving the data, **Fig. 4; ¶ 24**); and

"the analyzer is configured to analyze also said additional data for identifying the missing information" (Rowland discloses that the passive analysis tool analyzes whether a specific port is active or not, **Fig. 2; ¶ 25**).

As to **claim 66**, Rowland discloses all of claim 64.

Rowland further discloses that "the analyzer is configured to analyze nodal information that includes operating system information relating to operating systems operating on the one or more detected node" (Rowland discloses the passive analysis tool analyzes the data received in response to the OS fingerprinting request, **Fig. 3; ¶ 30-31**).

As to **claim 67**, Rowland discloses all of claim 66.

Rowland further discloses "the detection of data conveyed by the one or more detected nodes comprises detecting at least one type of message from a group comprising DHCP (Dynamic Host Configuration Protocol) messages and SYN packets." (Rowland discloses monitoring data packets from the DHCP server, **Fig. 4; ¶ 34**).

As to **claim 68**, Rowland discloses the network information collector of claim 66 and further discloses:

"an input device configured to receive data, giving rise to the detected data, the data corresponds to data conveyed by a detected node" (Rowland discloses obtaining ("receiving") OS information from a known ("detected") target address, (**¶ 37**);

"a data inspector coupled to said input device, the data inspector being configured to inspect said received data for one or more characteristics of a known operating system" (Rowland discloses a passive analysis tool that will receive and analyze the data to detect the OS of a target node, **Fig. 4, ¶ 37 and 24**); and

"a data marker coupled to said data inspector and being responsive thereto, the data marker being configured to indicate that the known operating system operates on the detected node" (Rowland discloses that the OS fingerprint for a target address is stored to indicate the known OS, **Fig. 4, ¶ 37**).

As to **claim 70**, Rowland discloses the network information collector of claim 64 and further discloses that the query engine includes:

"a query message generator configured to generate a query message corresponding to the missing information for conveying said query message to nodes to be queried" (Rowland discloses an OS fingerprinting mechanism that sends IP packets to the target host in order to retrieve the information; **¶ 24**) ; and

""an output device configured to convey the query message to the nodes to be queried, giving rise to the queried nodes" (Rowland discloses that the passive analysis tool initiates the OS fingerprinting query, **¶ 30**).

As to **claim 71**, Rowland discloses the network information collector of claim 70 and further discloses the query engine includes:

"an input device configured to receive at least one response that corresponds to the query message" (the OS fingerprinting method obtains, or receives, the information in response to querying the target host (**¶ 37**); and

"a response processor configured to process said at least one response to retrieve information corresponding to the missing information" (Rowland discloses the ability to handle the received response to the OS query and store the information, **¶ 37**).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. **Claim 59** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Rowland (US PGPub US2003/0212910)** in view of **Keir et al. (US PGPub 2004/0078384)** (hereinafter Keir).

As to **claim 59**, Rowland discloses all of claim 57 as described in paragraph 3 above.

Rowland does not disclose "the query message is one of the following: an ARP (Address Resolution Protocol) request; an ICMP (Internet Control MessageProtocol) echo request; and a TCP-SYN request".

Keir et al. teaches an operating system fingerprinting method by sending TCP SYN packets to the target computer **(¶ 97).**

Keir et al. and Rowland are analogous art as they both pertain to obtaining fingerprints of a communication network.

It would have been obvious to one skilled in the art at the time the invention was made to use the TCP-SYN message with the fingerprint method in Rowland being that, as Keir et al. states in ¶ 96, the network strain is significantly reduced during detection of the operating systems of a large number of target computers on a target network.

10. **Claim 55 and 56** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Rowland (US PGPub US2003/0212910)** in view of **Tonelli et al. (US Patent 5,821,937)** (hereinafter Tonelli).

As to **claim 55**, Rowland discloses all of claim 47 as described in paragraph 3 above.

Rowland does not teach "nodal information comprises hardware information relating to hardware components associated with the respective detected nodes".

Tonelli teaches a query engine that obtains network information from probes. The SNMP probe gathers IP and media access control (MAC) address information from the devices **(col. 19, lines 31-38)**.

Tonelli and Rowland are analogous art because they both deal with auditing network devices and collecting network information.

It would have been obvious to one skilled in the art at the time the invention was made to use the probe in Tonelli with the method of Rowland in order to discover hardware information associated with a network device.

As to **claim 56**, Rowland discloses all of claim 47 as described in paragraph 3 above.

Rowland does not teach "the nodal information comprises topology information relating to physical topology of the communication network".

Tonelli teaches a query engine that obtains network topology information from probes. (**col. 18, lines 35-45**). It would have been obvious to one skilled in the art at the time the invention was made to use one of the probes in Tonelli with the method in Rowland in order to detect topology information.

Additionally, applicant admits prior art in ¶ 103 of the instant application in which there are known methods for determining topology of a network based on data detected on that network.

11. **Claim 53, 54, 60-62 and 69** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Rowland (US PGPub US2003/0212910)** in view of **Thorpe et. al (US 7,089,306)** (hereinafter Thorpe).

As to **claim 53**, Rowland discloses all of claim 47.

Rowland does not teach that nodal information comprises "runtime information relating to running processes."

Thorpe teaches a process to use fingerprints to allow network and computer assets to be discovered, including installed software, and which software processes are in execution (**Fig. 19A-B; col. 20, lines 54-67; col. 21, lines 1-4**).

Rowland and Thorpe are analogous art in that they both pertain to fingerprinting systems in a network.

It would have been obvious to one skilled in the art at the time the invention was made to use the method of detecting running processes in Thorpe with the fingerprinting method of Rowland being that once the operating system has been fingerprinted, additional information may be discovered by sending operating system specific queries to the node.

As to **claim 54**, Rowland discloses all of claim 47.

Rowland does not teach that nodal information comprises "runtime information relating to running processes include at least one of the following: information relating to network running processes operating on the detected nodes and information relating to local running processes operating on the detected nodes".

Thorpe teaches a process to use fingerprints of discovered ("detected") computers to further discover the installed software and the processes which are in execution on a particular computer ("local running processes") (**col. 20, lines 54-67; col. 21, lines 1-4**).

For the same reasons stated above for claim 53, it would have been obvious to one skilled in the art at the time the invention was made to use method of detecting running processes in Thorpe with the fingerprinting method of Rowland.

As to **claim 62**, Rowland discloses all of claim 57.

Rowland does not disclose "missing information relates to at least one running process operating on respective queried nodes".

Thorpe teaches that software processes in execution are discovered by invoking function calls of ("querying") the operating system detected by fingerprinting (**col. 21, lines 1-4 and 28-35**).

For the same reasons stated above for claim 53, it would have been obvious to one skilled in the art at the time the invention was made to use method of detecting running processes in Thorpe with the fingerprinting method of Rowland.

As to **claim 69**, Rowland discloses all of claim 64.

Rowland does not disclose that the analyzer is "configured to analyze nodal information that comprises runtime information relating to running processes".

Thorpe teaches a method to gather information from a system that has been fingerprinted, which includes information on processes executing on the system, then receives and stores the information in a table and may assess the probability that the information exists (**Fig. 19C-step 150; col. 24, lines**).

For the same reasons stated above for claim 53, it would have been obvious to one skilled in the art at the time the invention was made to use method of detecting running processes in Thorpe with the fingerprinting method of Rowland.

As to **claim 60**, Rowland discloses all of claim 57.

Rowland does not teach "the generating is done in accordance with a test policy and wherein the test policy is selected from a group of available test policies".

Thorpe teaches a set of collection instructions defining what types of information can be gathered fro each source or node and the rules, i.e. methods and protocols, of doing so (**Figs. 15; col. 18, lines 18-57**).

It would have been obvious to one skilled in the art at the time the invention was made to use the collection instructions in Thorpe with the fingerprinting method of Rowland being that it allows additional information to be gathered from a node based on the results of the operating system fingerprinting.

As to **claim 61**, Rowland discloses all of claim 57.

Rowland does not disclose that generating a query message "is done in accordance with a test policy and wherein the test policy is selected in accordance with a statistical computation".

Thorpe discloses a method where the probably of the existence of an attribute based on the probably of the existence of an attribute ("nodal information") by computing an average of weighting factors returned from processing some of the rules (**Fig. 18A-B; col. 20, lines 32-48**).

For the same reasons stated above for claim 60, it would have been obvious to one skilled in the art at the time the invention was made to use the method of detecting running processes in Thorpe with the fingerprinting method of Rowland.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARIA L. SEKUL whose telephone number is (571)270-7636. The examiner can normally be reached on Monday - Friday 9:00-5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MARIA L. SEKUL
Examiner
Art Unit 2461

/Dmitry H. Levitan/
Primary Examiner, Art Unit 2461